IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATA MENGGUNAKAN AES (Studi Kasus Baitul Maal wat-Tamwil Al Ittihad Kota Pekanbaru)

Ardiasyah[1)], Harun Mukhtar [2)]
[1)]ProgramStudiTeknik InformatikaFakultasIlmu Komputer, UniversitasMuhammadiyah Riau
Ardhiansyah@gmail.com
[2)]ProgramStudiTeknik InformatikaFakultasIlmu Komputer, UniversitasMuhammadiyah Riau
harunmukhtar@umri.ac.id

Abstract

The issue of security and confidentiality of data and information is an important matter. One way to maintain the security and confidentiality of data and information is by encryption and decryption techniques, also known as cryptography. Cryptography is the science and art of maintaining message security by turning it into a form that cannot be recognized anymore. One cryptographic algorithm that is often used today is Rijndael or also known as AES (Advanced Encryption Standard). Cryptography can be applied to various types of files, one of which is a customer data document. The software to be built is encryption and decryption software with the Rijndael algorithm for customer data documents. The results of this study are: applications that are designed to meet information security needs, both protection of the confidentiality of information and protection against falsification and alteration of unwanted information.

Keywords: *Cryptography,AES,data security, customer data*

Abstrak

Masalah keamanan dan kerahasiaan data dan informasi merupakan suatu hal yang penting. Salah satu cara menjaga keamanan dan kerahasiaan data dan informasi adalah dengan teknik enkripsi dan dekripsi atau yang dikenal juga dengan kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara mengubahnya menjadi suatu bentuk yang tidak dapat dikenali lagi. Salah satu algoritma kriptografi yang sering digunakan saat ini adalah Rijndael atau yang dikenal juga dengan AES (Advanced Encryption Standard). Kriptografi dapat diterapkan pada berbagai jenis file, salah satunya adalah dokumen data nasabah. Perangkat lunak yang akan dibangun adalah perangkat lunak enkripsi dan dekripsi dengan algoritma Rijndael untuk dokumen data nasabah. Hasil dari penelitian ini ada;ah aplikasi yang dirancang mampu memenuhi kebutuhan keamanan informasi, baik perlindungan terhadap kerahasiaan informasi maupun perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan.

***Kata Kunci**:* Kriptografi, AES, keamanan data, data nasabah
.

1. Pendahuluan

Banyak aspek yang harus diperhatikan dalam mendukung penyediaan layanan tersebut antara lain Pengembangan Sistem Perbankan (Development of Banking System), Pengembangan Sistem Informasi (Development of Information System), penyediaan hardware yang memadai, dan tak kalah penting adalah Pengembangan Keamanan Sistem Informasi (Development of Information Security System), yaitu keamanan yang memberikan perlindungan baik bagi sistemnya sendiri, maupun terhadap aset Baitul Maal wat-Tamwil (BMT) berupa data yang ada meliputi data intern, data nasabah dan data transaksi. Pengamanan dan perlindungan tersebut dilaksanakan tidak hanya secara fisik tetapi juga dengan pemanfaatan kemajuan teknologi informasi. Masalah yang banyak dibicarakan dalam jaringan global adalah bagaimana memberikan keamanan tehadap data dan informasi karena menyangkut kepentingan pribadi, institusi, keamanan negara dan perusahaan. Oleh karena itu banyak negara-negara yang maju yang telah menghabiskan dana berjuta-juta untuk menangani dengan serius keamanan komunikasi yang sangat

rahasia, terutama informasi yang menyangkut tentang kekuatan agen rahasia negara atau hal-hal yang

menyangkut rahasia orang yang melakukan aktifitas di jaringan komputer global

Oleh karena itu perlu adanya metode yang memberikan keamanan terhadap data dan informasi dari kebocoran terhadap orang lain yang tidak mempunyai wewenang untuk mengetahuinya. Salah satu cara untuk menjaga keamanan dan kerahasian suatu data maupun informasi adalah dengan teknik enkripsi dan dekripsi guna membuat data ataupun informasi yang disimpan tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk pihak yang berwenang terhadap data tersebut. Teknik pengamanan data dan informasi dengan enkripsi dan dekripsi dikenal dengan Kriptografi. Berbagai macam algoritme Kriptografi dapat diimplementasikan untuk mewujudkan sistem keamanan data. Diantaranya yaitu algoritme Kriptografi Salah satunya dengan menggunakan metode algoritme Advanced Encryption Standard (AES). (Pabokory et al., 2015). Dari permasalah pada latar belakang di dapatkan identifikasi masalah : Data-data nasabah sangat rentan untuk dapat disalah gunakan oleh pihak yang tidak bertanggung jawab. Data nasabah seperti Nama, Nomor NIK KTP, NIK KK, dan Nama sering disalah gunakan untuk keperluan pribadi sehingga nasabah sering dirugikan. Dalam Penelitian ini, masalah yang akan dibahas adalah : Bagaimana membuat perangkat lunak enkripsi dan dekripsi untuk menjaga keamanan data nasabah. Bagaimana menerapkan Metode AES *(Advanced Encryption Standard*) untuk mengenkripsi data nasabah.

1) Tujuan Penelitian, implementasi enkripsi data nasabah menggunakan Metode *Algoritme* AES pada BMT Al-Ittihad

2) Batasan Masalah Penelitian ini, Data yang akan dienkripsi maupun di dekripsi berbentuk file. File tersebut berupa dokumen seperti Ms Exel(.xlsx), *Plainteks* yang akan di enkripsi dan dekripsi hanya 146 orang nama anggota nasabah *BMT Al-Ittihad*.146 orang data nasabah yang akan di enkripsi karena jika aplikasi sudah berjalan dengan baik, maka seluruh data-data nasabah akan di enkripsi oleh pihak BMT.

2. Metodologi Penelitian

Untuk hasil yang lebih maksimal, berikut ini adalah metodologi yang digunakan untuk kegiatan, dan prosedur yang digunakan dalam penyusunan skripsi yaitu menegenai bagaimana perancangan sistem kriptografi pengamanan data dengan menggunaka *algoritme* AES.

a. Pengumpulan Data, pengumpulan data dilakukan untuk mendapatkan data-data BMT yang akan di sandikan
b. Analisis data, mengelompokan data yang akan disandikan berdasarkan kriteria kesamaan data dan penguna data
c. Perancangan Sistem, sistem kriptograpy dibangun berbasis desktop
d. Implementasi sistem
e. Pengujian Sistem

3. Hasil dan Pembahasan

a. Analisis

Pada tahap analisis,dilakukan penguraian serta penjelasan terhadap topik penelitian yang berguna untuk mengidentifikasi dan mengevaluasi proses-proses,serta kebutuhan yang diperlukan agar dapat diusulkan suatu solusi untuk diterapkan pada tahap peancangan. Penjabaran serta penjelasan dari tahap analisis akan dikelompokkan menjadi dua bagian, yaitu analisis proses dan analisis kebutuhan.

1) Analisis Proses

Analisis proses merupakan tahapan dimana dilakukannya proses pembangkitan kunci yang akan digunakan sebagai kunci *private*. Selain itu didalam analisis proses ini juga terdapat analisis proses enkripsi file, dan juga proses dekripsi terhadap file yang sebelumnya telah di*enkripsi*. Berikut adalah penjelasan mengenai langkah tersebut.

2) Proses Enkripsi (*Encryption*)

Proses *enkripsi* diawali dengan memilih *document (*file) yang akan dienkripsi. Setelah di tentukan letak penyimpanan dokumen yang setelah dienkrip tersebut, proses berlanjut pada masukan kunci/*password*, proses dilanjutkan dengan proses enkripsi. Hasil dari proses enkripsi berupa *Chipertex* Proses Perhitungan Enkripsi

Plain Text : Universitas Muhammadiyah

Chiper Key 2014000000000000

Masukkan Ke Kolom 4 X 4

3) Skenario Implementasi

Skenario implementasi dimulai pada menu utama program, pertama sekali pogram dijalankan akan menampilkan menu utama program, selanjutnya masukan dokumen yang akan dienkripsi, setelah itu masukan *passwod*nya. Langkah selanjutnya klick *icon Encrypt*, selanjutnya akan muncul notifikasi bahwa proses *encrypt* berhasil dan hasilnya bisa dilihat pada *direktory* tempat kita simpan dokumen hasil enkripsi.
Langkah terakhir dari perintah ini adalah memasukan kata sandi/*password* serta dokumen yang akan didekripsikan, kemudian untuk memulai proses

dekripsi klik tombol *Decrypt* hasil program ini akan terlihat pada *diektori* dimana kita simpan hasil dekripsi tersebut.

4) Implementasi Skenario

Implementasi Skenario merupakan tahap pembuatan aplikasi berdasarkan hasil analisa dan perancangan sistem sebelumnya, sehingga sistem yang dibuat dapat difungsikan dalam keadaan sebenarnya dan sesuai dengan tujuan yang diharapkan. Implementasi sistem ini dilakukan setelah proses perancangan dan kodingan selesai. Dimana didalam implementasi ini sistem dijalankan dan diamati untuk melihat kinerja yang dimilikinya. Berikut ini adalah implementasi untuk setiap proses yang ada pada sistem kriptografi AES

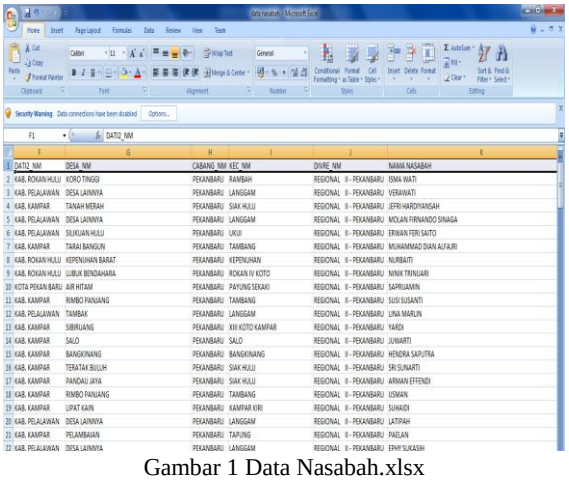
b. **Pengujian**

1) Pengujian Program

Pada uji kali ini dilakukan proses enkripsi, dan dekripsi terhadap dokumen yang akan dienkrip. Menggunakan program yang telah dibuat.

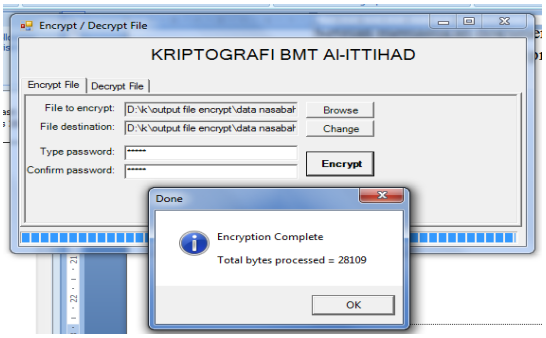
2) Proses Enkripsi

Sebelum melakukan *enkripsi* dokumen, pengguna harus memilih browse/pilih dokumen yang kan dienkripsi, dokumen yang akan di uji yaitu dokumen berektensi.xlsx. dokumen ini berisi tentang data-data nasabah sehingga kategori isi file tersebut besifat rahasia. Berikut adalah contoh dokumen datanasabah.xlsx. seperti terlihat pada gambar 1 berikut



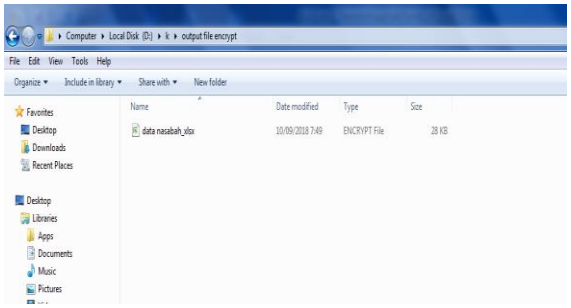
Gambar 1 Data Nasabah.xlsx

Setelah memasukan dokumen yang akan dienkripsi, maka proses enkripsi dapat dilakukan.dan gambar dari proses enkripsi, dapat dlihat pada gambar 2



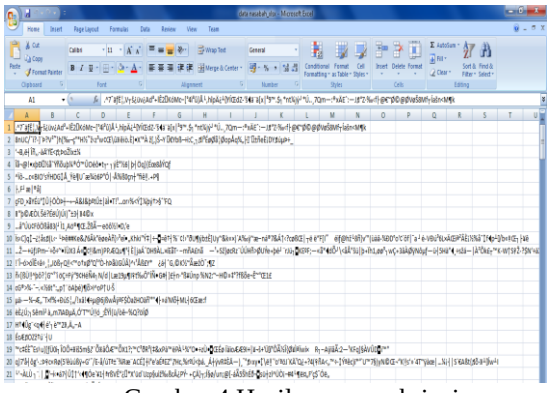
Gambar 2 Proses Enkripsi

Adapun output dari hasil enkrip tersebut,adalah dokumen enkripsi yang berektensi *encrypt file*. Adapun gambar output hasil enkripsi dapat dilihat pada gambar 3



Gambar 3 *Output* hasil enkripsi

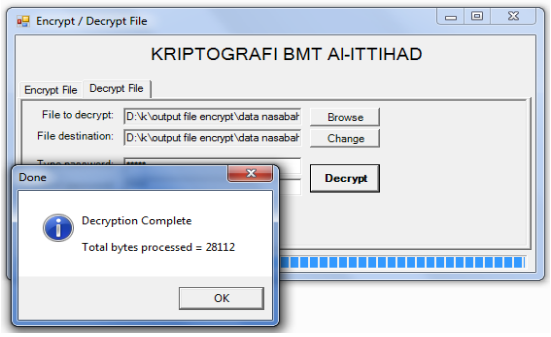
Setelah proses enkripsi berhasil dilakukan, maka dokumen yang tadinya berisi mengenai data nasabah dengan teks yang dapat dibaca, sekarang dokumen tersebut menjadi teks yang tidak dapat dibaca. Adapun gambar dari hasil proses enkripsi dapat dilihat pada gambar 4



Gambar 4 Hasil proses enkripsi

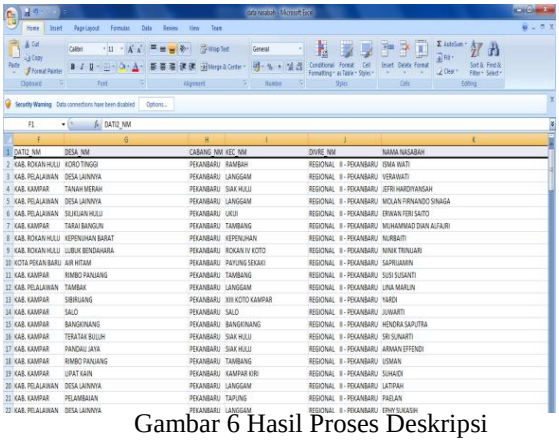
3) Proses Dekripsi

Untuk melakukan proses dekripsi, pengguna terlebih dahulu harus memasukan dokumen yang telah dienkripsi sebelumnya. Adapun gambar proses dekripsi dapat dilihat pada gambar 5



Gambar 5 Tampilan proses dekripsi

Setelah proses dekripsi berhasil dilakukan maka dokumen yang tadinya berisi mengenai data nasabah dengan teks yang tidak dapat dibaca, sekarang dokumen tersebut kembali menjadi teks yang dapat dibaca. Adapun gambar dari hasil proses dekipsi dapat dilihat pada gambar 6



Gambar 6 Hasil Proses Deskripsi

4. **Kesimpulan**

a. Kesimpulan

Berdasarkan hasil penelitian dan pengujian sistem enkripsi data nasabah yang telah dilakukan oleh penulis, maka dapat diambil beberapa kesimpulan yaitu:

1) Penelitian ini berhasil membangun sebuah sistem kriptografi pada BMT Al-ITTIHAD Pekanbaru.
2) Dengan menggunakan *algoritme* AES, dapat digunakan untuk menjaga kerahasiaan informasi data sekaligus dapat mencegah penyalah gunaan data oleh pihak yang tidak bertanggung jawab
3) Penggunaan kunci merupakan sesuatu yang sangat penting dalam proses enkripsi dan dekripsi, sehingga dibutuhkan suatu kerahasiaan dalam pemakaian kuncinya.
4) Penerapan aplikasi kriptografi ini dikomputer *standalone*, karena Bersifat personal (hanya untuk kalangan sendiri).

b. Saran

Setelah mengamati dan menganalisa pemasalahan yang ada, maka ada beberapa saran untuk mengembangkan sistem yang telah ada agar lebih baik, yaitu:

1) Harus diberikan pengetahuan tentang enkripsi dan dekripsi kepada *user* di BMT Al-ITTIHAD Pekanbaru
2) Dihaapkan untuk penelitian selanjutnya, agar dapat mengenkripsi lebih dari satu dokumen sekali enkripsi.

Daftar Rujukan

[1] Busran, & Putra Novernus Ayundha. (2014). Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Rsa Pada Sistem Keamanan File Berbasis Javaeknoif. *Jurnal Teknoif*, *2*(1), 7–17.

[2] Febriana, I., S, G. A., & Informasi, P. T. (2017). Penerapan Teknik Kriptografi Pada Keamanan Smsandroid, *1*, 29–36.

[3] Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi Rsa Untuk Enkripsi Dan Dekripsi Email. *Jurnal Teknologi Dan Sistem Komputer*, *3*(2), 253.

[4] Mukhtar, H. (2010). Penerapan Kriptografi Untuk Keamanan Data